AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
Western District of Arkansas
Hot Springs Division

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH SEVEN FACEBOOK ACCOUNTS, THAT ARE STORED AT PREMISES CONTROLLED BY FACEBOOK, INC.

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH TWO GOOGLE ACCOUNTS, THAT ARE STORED AT PREMISES CONTROLLED BY GOOGLE LLC

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH TWO WHATSAPP ACCOUNTS, THAT ARE STORED AT PREMISES CONTROLLED BY WHATSAPP

Case No. 6:19-CM-03

Filed Under Seal

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe property to be searched and give its location):*
See "Attachment A"

located in the Western District of Arkansas, there is now concealed *(identify the person or describe the property to be seized)*:
See "Attachment B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

X evidence of a crime;

☐ contraband, fruits of crime, or other items illegally possessed;

☐ property designed for use, intended for use, or used in committing a crime;

☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18, United States Code, Section 1591	Sex Trafficking of Children or by Force, Fraud, or Coercion

The application is based on these facts:

X Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Katie C. Rowbotham, Special Agent, FBI

Sworn to before me and signed in my presence.

Date: 2-21-19

Judge's signature

City and state: ~~Hot Springs~~, Texarkana, Arkansas

Barry A. Bryant, United States Magistrate Judge

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF ARKANSAS

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH SEVEN FACEBOOK ACCOUNTS, THAT ARE STORED AT PREMISES CONTROLLED BY FACEBOOK, INC. IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH TWO GOOGLE ACCOUNTS, THAT ARE STORED AT PREMISES CONTROLLED BY GOOGLE LLC IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH TWO WHATSAPP ACCOUNTS, THAT ARE STORED AT PREMISES CONTROLLED BY WHATSAPP	Case No. 6:19-CM-03 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Katie Rowbotham, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for search warrants under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) for information associated with Facebook user ID numbers: **100026170149068, 100013269482917, 100009344742059, 100025340801469, 100028908998220**, **100024430478019,** and **100014475964292** that are stored at premises owned, maintained, controlled, or operated by Facebook Inc. (Facebook), a social networking company headquartered in Menlo Park, California; information associated with **allooper2600@gmail.com** and **allhiswill2600@gmail.com**, that are stored at premises owned, maintained, controlled, or operated by Google LLC, an electronic communication service provider located in Mountain View, California; information associated with the WhatsApp

accounts with **allooper2600@gmail.com** and **allhiswill2600@gmail.com,** that are stored at premises owned, maintained, controlled, or operated by WhatsApp, an electronic communication service provider located in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A.

2. I am a Special Agent of the Federal Bureau of Investigation (FBI) and have been a Special Agent since March 2013. I was previously employed with the National Park Service as a Federal Law Enforcement Officer and as an Officer in the United States Marine Corps. I am currently assigned to the Little Rock, Arkansas, Field Office as a member of the Joint Terrorism Task Force (JTTF). My primary duties are to conduct criminal investigations involving domestic terrorism investigations, illegal possession, distribution, and manufacture of controlled substances and violent crimes against children, to include human trafficking, child prostitution, and production of child pornography. I have received training in the area of investigating child pornography and child exploitation. I have had the opportunity to observe and review numerous electronic wire communications such as emails and text messages that involve the sexual exploitation of minors, specifically, 18 U. S. C. § 1591(a)(1) (interstate sex trafficking of persons who have not attained the age of 18 years). As a federal law enforcement officer engaged in enforcing criminal laws, I am authorized by the Attorney General to request a search warrant.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this investigation.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U. S. C. § 1591 may have been committed

by Aaron Looper in the Western District of Arkansas, Hot Springs Division and elsewhere. There is also probable cause to search the information contained within Attachment A for evidence, instrumentalities, contraband or fruits of these crimes, as further described in Attachments B.

PROBABLE CAUSE

1. On or around May 1, 2018, Captain Gary Ashcraft with the Garland County, Arkansas, Sheriff's Department (GCSD) was contacted by Clarence Glenn (Glenn) in reference to the possible trafficking and prostitution of females including minors.

2. Captain Ashcraft and Lieutenant (Lt.) Joel Ware contacted Glenn at Lone Wolf Auto Body where Glenn was employed. Glenn showed officers text messages he had received over Facebook around July 2018 from an individual identified as Aaron Looper (Looper). Looper sent Facebook messages to Glenn referencing how Looper liked really young girls that were new to the dope game. Looper stated his preference for young girls like his 17-year-old niece. Looper sent photographic examples of the women he liked to Glenn. Those photographs included nude, semi-nude, and clothed females. According to Lt. Ware, some photos were of nude, white females who appeared to be of pre-pubescent age. Lt. Ware described one photograph was a girl who appeared to be less than 12 years old and was unclothed from the waist up.

3. The photo associated with the Facebook account of Looper was a still image of Looper's face. Looper's Facebook account was identified as Facebook ID **100026170149068**.

4. On August 1, 2018, Glenn was taken into custody on a parole violation. His cellular telephone was seized and reviewed pursuant to his parole agreement. Parole officers saw photographs on Glenn's cellular telephone of clothed and nude females who appeared to be

minors.

5. Your Affiant received information from a Confidential Human Source (CHS) regarding Looper's involvement with the White Aryan Resistance (WAR) and human trafficking around Hot Springs, Arkansas. The CHS explained that WAR members kidnap women and sell them for sex. Some of the women are recruited to assist in drug trafficking. Some of the women are sold and sent to other states to work for other members of WAR. The group members brand the women with swastikas to show they are owned. If the women don't do what they are told, they receive punishments like getting their heads shaved. Many of the women are posted on Internet sites like Backpage.com, but most are solicited via word of mouth.

6. Your Affiant's research indicates that in 2011, FBI Little Rock received CHS reports Looper was associated with a white supremacist group affiliated with the Aryan Nation and the sexual assault of a teenage girl. According to the CHS, Looper also cut a swastika in the girl's body. The underage girl's name was revealed in the report. According to the CHS, Looper told the CHS that Looper had killed two teenage boys because they were going to testify against him for the incident with the young girl. The CHS provided details of the location and date of the incident.

7. Based on the above information, a search warrant, issued in the United States District Court for the Western District of Arkansas on August 30, 2018, for Facebook user name Aaron Looper ID **100025340801469**, was executed via Facebook online portal on August 30, 2018. Evidence obtained from that search warrant was received September 30, 2018. The registered email associated with the Facebook account was **allooper2600@gmail.com**. The Facebook account was created four months prior to the search warrant execution.

8. Your Affiant conducted a review of digital evidence returned from Facebook

pursuant to the search warrant for user Aaron Looper ID **100025340801469** and found that Aaron Looper had multiple conversations discussing kidnapping young girls in conversations on Google Hangouts, WhatsApp, Google drive, and Gmail. Specifically, Looper sent a Facebook message to T. B. in which Looper expressed his desire to kidnap and drug a "real young dumb" girl. Looper sent a Facebook message to B. B. about drugging women and invited B. B. to join him. Looper stated, "We need to kidnap drug and fuk [sic] a girl." Looper had a Facebook conversation with a CHS where Looper stated, "I wana young pretty runaway or something for us to video." Looper also discussed his desire to have CHS have sex with MINOR 2.

9. From June 26, 2018, to September 7, 2018, Looper (hereinafter referred to as "AL" for purposes of identifying participants in the Facebook conversation) using Facebook user ID **100026170149068,** had the following Facebook Conversation with T. B. (TB) regarding selling drugs and kidnapping a young girl:

AL: Where the real nasty whores at

TB: I don't know Aaron I'm clean but I like nasty whores

AL: I got drugs cash and it that don't work I got duktape. U stay clean I'll get one spun and fuked up or pay cash for her to let us both fuk her

TB: (thumbs up)

AL: I'll for real kidnap one if we know when and where she be. For real young dumb give first shot and fuk

TB: Bet that

AL: Swearbgetba good one and know her address and when she alone I'll shott up the youngest girl and us both do her to dewth

TB: Already bro hit me up I got to go to work

…

AL: Any ideals? Lik savanna or some lil good girl

TB: Let me go through my phone I don't think Savannah is going though I don't even know where she's at

AL: Ok. Find a good lil girl or sober one or young as hell we can kidnap. For real

TB: Ok

AL: Don't forget even if I got kidnap em for real

TB: cool

AL: Preferably young and dumb

TB: (thumbs up)

TB: What about [MINOR 1]

AL: Fuk yeah she work

AL: Give her 100 in nek and do her

TB: Let me see what I can do

10. From May 2, 2018, to September 7, 2018, B. B. (BB) had the following Facebook conversation with Looper's Facebook user ID **100026170149068,** regarding kidnapping and drugging young girls:

AL: U need can ful this mixed bigger girl

AL: Nigger

AL: She young and shoots meth and loves fumed like nigger

AL: Wanna join

AL: Now

BB: YEA CAN YOU COME GET ME

AL: (Sends picture of multiple young women and a picture of an unknown female's vagina).

…

BB: do you have anything 4 sale

AL: How much c h

BB: 100

AL: It's from another state all I can do is gram and half for 80 or 2 for 100

BB: Can you bring it to me

BB: hello

AL: Yes my girl in the shower and then I will

AL: C u in hour or less

BB: ok I got a 100 bill

BB: se you soon

AL: (send thumbs up)

AL: We need to kidnap drug and fuk a girl

BB: hey are you o youre waay

BB: alright

BB: are moble yet

AL: (sends thumbs up)

…

11. On February 2, 2019, Looper's Facebook user ID **100028908998220** and a CHS had the following Facebook and email conversation using **allhiswill2600@gmail.com** regarding kidnapping a young girl:

AL: Shoilds seen my victim last night

CHS: Kh yes tell me

AL: AL: Shoilds seen my victim last night

CHS: Kh yes tell me

AL: Young mex girlil bring pics

CHS: How young you think

AL: 16

CHS: You should just bring her down. I want to see what she looks like.

AL: I'll end pic soon and bet. She halfnex quarter blak and quarter white. He dad knows and I will lo e the way she forces herself to please

AL: Not her (sends link to unknown picture/video)

CHS: Oh yes looks like my kind of party. Can't wait to see more. I have not had any real excitement in a

AL: Our excitement will be best ever. I wana young pretty runaway or something for us to video

CHS: I'm sure we can find one. Nothing a little dope can't by!!

AL: Right I want one from town away from u or e so I can break her and sell her

CHS: We can go to Baton Rouge or New Orleans. Good time of year with martigras coming up

AL: Fuk yeah. U know im really wana break her on video and sel her when done??

CHS: I got a good camera

AL: Like good nuff we wear mask and get em super high and shit and s are em while breaking them on video bc we can make a bindle on her

…

AL: Like young small girl while mom watches then her

…

AL: And realy id love c u fuk my daughter (MINOR 2)

CHS: Oh yes what's she like

AL: Look her facebook (MINOR 2) So hot and would do it

CHS: OK I'm going to take me a look. Have you got to turn her out yet

AL: I gave her first shot after her mom turnrd get out and she watched me

....

12. On February 3, 2019, Looper asked CHS for his/her email address. Looper shared one video with the CHS via Google photos associated with Google account **allhiswill2600@gmail.com**. The video depicted an adult male and an unknown aged female engaged in sexual activity. The unknown female also had a syringe in her arm with what appeared to be an injection of a controlled substance. CHS stated Looper sent the video to show activities Looper was interested in sexually. Looper continued the Facebook conversation about wanting to rape MINOR 2 and sell her.

13. On February 9, 2019, your Affiant located and interviewed MINOR 2, a 16-year-old. MINOR 2 stated she believed Looper might be her biological father and that he recently contacted her via Facebook (UserID **100024430478019)** in October, 2018 when he wrote: "Addme on this account as ur dad and friend please. Hipe u ok. I wana see u badly. Maybe for Christmas."

14. MINOR 2 stated she hadn't seen Looper in five years and didn't know if she would be able to see him. MINOR 2 also stated she didn't want to be around him if he was using drugs. In December, 2018, Looper told MINOR 2 he wanted to send her money and MINOR 2 gave him her home address. During your Affiant's interview of MINOR 2, MINOR 2 stated Looper sent her a $30 gift card in January 2019, but nothing in February 2019. MINOR 2 stated

Looper had multiple Facebook accounts and explained Looper would use one account for a while and then use another for a different time period. Your Affiant observed two Looper profiles under MINOR 2's Facebook friends.

15. From March 2017, to February 11, 2019, Looper's Facebook user ID **100014475964292** had Facebook conversations with a CHS. Looper sent multiple pictures of women of unknown ages and photographs of female and male genitalia. On February 9, 2019, Looper wrote: "Laying here my other account locked me out so ….and my text number stil works 5018076677. Save that. Anyways just sitting here what u doin."

16. On February 7, 2019, Looper's Facebook user ID **100028908998220** had a Facebook conversation with a CHS. Loooper sent five pictures of clothed teenage girls to CHS, talked about making porn, and stated he was currently communicating with two "new girls." Portions of the conversation are as follows:

CHS: Is that your atep daughter

AL: Fuk I wish. If so id already have millions bc wed make a whole seriesof porns of her and id keep her pregnant with help from guys and me and u would both fuk all her holes and id watch as her eyes dimmed and she stoped breathing. On an altear"

CHS: Blood sacrifice!! We would be so blessed. And I have to say after my entertainment with the mini porn I was like is that you cause your ass has demples. And that's the girl we gonna breed first ?? I been thinking all about it

AL: The video aint me. And that new girls two pics toda is a lil who're im chatting with on fbook

17. From May 31, 2018, to June 12, 2018, Looper's Facebook user ID **100026170149068** had the following Facebook conversation with D. B. (DB) regarding sex with

someone's daughter. Looper did not want to send pictures over Facebook, only text. Portions of those text conversations appear verbatim as follows:

AL: Fuck my wife

AL: (sends thumbs up)

DB: Yh

AL: I seearbto good I'll ziptie her give her a big shit of meth and force her to swallow u whole and hold her down alllway till u allow her to breath

DB: Woo-hoo

DB: I'll force my 11inches thick dick fully in her ass till she cry

AL: And let's use her daughter like I do

DB: Wow

AL: She good Lil whore

DB: Send me her pictures

AL: And loves getting high and helping punish her mom

AL: Can I text u pics?

DB: Yed

DB: Yes

AL: Need phone number

DB: Send it here

AL: I cant

DB: Y?

AL: Not online text only

AL: (sends thumbs up)

Al: I'm high and thinking of u

AL: What number

DB: +233545170715

DB: Send pics

AL: (sends thumb up)

AL: She want it bad

BD: Let me see her pussy

AL: K

18. From August 21, 2018, to September 7, 2018, Looper Facebook user ID **100026170149068** had the following conversation with M. M. (MM) regarding making pornography and AL discussed storing homemade pornography on his google drive account:

…

MM: Where the Gfreeks

MM: (Sends picture of a clothed female who appears to be around 16-20 years of age)

AL: Fuki wish I knew

AL: Damn who she

MM: This is who I had over and did not have the right sheets on

MM: Chick from town

AL: Idtry break that lil broad

MM: U never send me tbe pic of dope hos

MM: I need homemade porn

AL: I can check my Google drive for some I have or we could startaking custom ones for cash

MM: Not your ass…..

AL: Duh

MM: I got lots

AL: I know peeps want local porn

MM: Ok I got

…

19. From May 1, 2018, to September 7, 2018 T. J. (TJ) had the following conversation with Looper Facebook user ID **100026170149068** regarding furthering their communication on WhatsApp user **allooper2600@gmail.com**:

TJ: hey

AL: Hey

AL: (sends thumbs up)

AL: Hot

AL: (sends photo of penis)

TJ: Nice to meet you

TJ: Where are you from

AL: Atkansas and u

TJ: Do you have WhatsApp number or hangout

TJ: West Africa

AL: Getting now

TJ: do you have WhatsApp number or hangout

AL: One min

TJ: Okey

AL: Ur name on whatsapp

TJ: lindarobert801@gmail.com

TJ: What happened

AL: Add me allooper2600@gmail.com

TJ; Okey

AL: Hurry

AL: U limemeth

TJ: I text you hangout now

...

20. From May 2, 2018, to September 7, 2018 A. J. (AJ) had a conversation with Looper Facebook user ID **100026170149068** regarding making porn and utilizing the messaging application Google Hangouts with user id **allhiswill2600@gmail.com.** Looper sent multiple pictures of an erect penis and AJ replied that he loved it. AJ asked if Looper had hangouts and Looper replied with the account **Allhiswill2600@gmail.com**. Looper talked about having sex with his 15 year old daughters and stated his job was to "make porn."

21. As of February 12, 2019, an open source search was completed on Facebook for accounts associated with the name Aaron Looper. Aaron Looper had the following Facebook pages and profile pictures associated with the account:

Facebook user ID **100026170149068**. Username "Aaron Looper." with a profile picture of a white male with dark background and appears to be Aaron Looper. This account was the basis of the original search warrant.

Facebook user ID **100013269482917.** Username "Aaron Looper" with a profile picture of a cartoon wolf and man sitting. The individual appeared to be from Hot Springs, Arkansas based on the listed information in the about section.

Facebook user ID **100009344742059.** Username "Aaron Looper" with a profile picture of a white male with plain background and appears to be Aaron Looper. The individual appeared to be from Hot Springs, Arkansas based on the listed information in the about section.

Facebook user ID **100025340801469.** Username "Aaron Looper" with a profile picture of a white male with plain background and appears to be Aaron Looper.

Facebook user ID **100028908998220.** Username "Aaron Looper" with a profile picture of a white male with dark background and appears to be Aaron Looper. The individual appeared to be from Hot Springs, Arkansas based on the listed information in the about section. This account was utilized during a conversation with a CHS.

Facebook user ID **100024430478019.** Username "Aaron Lee (Aaron Lee Looper)" has no profile picture, but pictures were observed in the profile in the past. The individual appeared to be living in Pearcy, Arkansas, and was from Hot Springs, Arkansas based on the listed information in the "about" section. This account was utilized during Looper's conversation with MINOR 2. This profile has changed profile pictures in the past.

Facebook user ID **100014475964292** Username "Aaron Looper: with a profile picture of a white male with plain background and appears to be Aaron Looper. The URL associated with the account is "Aryaninthespafortheabcs" This account was utilized during a conversation with a CHS.

22. Based on my training, experience, and knowledge of this investigation, I believe the content of the text conversations set forth in this Affidavit between Aaron Looper and other individuals set forth in pertinent part in this Affidavit are evidence of Looper's intent to produce child pornography, in violation of 18 U.S.C. § 2251; attempt distribute and distribution of child pornography, in violation of 18 U.S.C. § 225; and to recruit, entice, harbor, transport, provide,

obtain, advertise, maintain, patronize or solicit a person who has not attained the age of 18 years to engage in a commercial sex act, in violation of 18 U.S.C. § 1591.

23. Based on my training and experience, individuals involved with child exploitation offenses routinely have their Facebook accounts blocked or disabled due to offensive content. Facebook policy requires users to either answer security questions or get help from Facebook friends that can provide a URL to retrieve a security code. While disabled or locked accounts are still visible, Facebook requires a minimum 24 hour waiting period before account changes or access to the account could occur. Based on my training and experience, due to this Facebook policy, many users have multiple Facebook accounts. Therefore, your Affiant believes that the following seven Facebook accounts known to your Affiant have been utilized by Looper to communicate his intent to commit violations of 18 U.S.C. §§ 2251, 2252 and 1591 and they are sought by this search warrant: **100026170149068, 100013269482917, 100009344742059, 100025340801469, 100028908998220, 100024430478019,** and **100014475964292.**

24. Based on your Affiant's experience, those involved in child pornography and trafficking minor girls, routinely advertise, promote and communicate with like-minded individuals via Internet websites like Facebook and private messaging platforms like WhatsApp and Hangouts.

THE SERVICE PROVIDERS

25. I have learned the following about Facebook.

a. Facebook owns and operates a free-access social networking website of the same name that can be accessed at http://www.facebook.com. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts

to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

b. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

c. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

d. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create

"lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

e. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

f. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, the photos and videos associated with a user's account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

g. Facebook users can exchange private messages on Facebook with other users. Those messages are stored by Facebook unless deleted by the user. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a chat feature that allows users to send and receive instant messages through Facebook Messenger. These chat communications are stored in the chat history for the account. Facebook also has Video and Voice Calling features, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

h. If a Facebook user does not want to interact with another user on Facebook, the first user can "block" the second user from seeing his or her account.

i. Facebook has a "like" feature that allows users to give positive feedback or connect to particular pages. Facebook users can "like" Facebook posts or updates, as well as webpages or content on third-party (*i.e.*, non-Facebook) websites. Facebook users can also become "fans" of particular Facebook pages.

j. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

k. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as "liking" a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page.

l. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

m. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications ("apps") on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user's access or use of that application may appear on the user's profile page.

n. Facebook also retains Internet Protocol ("IP") logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user's IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

o. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records

of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

p. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-

location into some of its services. Geo-location allows, for example, users to "tag" their location in posts and Facebook "friends" to locate each other. This geographic and timeline information may tend to either inculpate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner's state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

q. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

26. I have learned the following about Google:

a. Google offers email services to the public. In particular, Google allows subscribers to maintain email accounts under the domain name gmail.com. A subscriber using Google's services can access his or her email account from any computer connected to the Internet.

b. Google maintains the following records and information with respect to every subscriber accounts.

i. *Email contents.* In general, any email (which can include attachments such as documents, images, and videos) sent to or from a subscriber's account, or stored in draft form in the account, is maintained on Google's servers

unless and until the subscriber deletes the email. If the subscriber does not delete the email, it can remain on Google's computers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google's servers for a certain period of time.

ii. *Address book.* Google allow subscribers to maintain the equivalent of an address book, comprising email addresses and other contact information of other email users.

iii. *Subscriber and billing information.* Google collects and maintains (typically unverified) identifying information about each subscriber, including, for example, name, username, address, telephone number, and alternate email addresses. Google also maintains records concerning the date on which the account was created, the IP address of the user at the time of account creation, the current status of the account, the length of service, and the types of services utilized by the subscriber. Additionally, for paying customers, Google maintains records of the subscriber's means and source of payment, including any credit card or bank account number.

iv. *Device information.* Google collects and maintains information identifying devices (including both computers and mobile devices) used to access accounts, including, for example, device serial number, a GUID or Global Unique Identifier, a phone number, MAC (media access control) addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Android ID, Subscriber Identity

Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI").

v. *Cookie Data.* Google uses features to track the activity of users of their accounts, including whether or not the user of an account accesses other accounts at Google using the same computer, or accesses accounts maintained by other companies while logged into an account. One of the ways they do that is by using cookies, a string of characters stored on the user's computer or web browser that is recognized by Google when a computer visits its site or logs into an account.

vi. *Transactional information.* Google typically retains certain transactional information about the use of each account on its system. This information can include records of login (i.e., session) times and durations and the methods used to connect to the account (such as logging into the account through Google's websites). Google retains information regarding accounts registered from the same IP address.

vii. *Customer correspondence.* Google maintains records of any customer service contacts with or about the subscriber, including any inquiries or complaints concerning the subscriber's account.

viii. *Preserved and backup records.* Google maintains preserved copies of the foregoing categories of records with respect to an account, for at least 90 days, upon receiving a preservation request from the Government pursuant

to 18 U.S.C. 2703(f). Google may also maintain backup copies of the foregoing categories of records pursuant to its own data retention policy.

In addition, Google maintains records with respect to other Google Services, which it stores in connection with subscriber accounts, which typically include the following:

ix. *Google Drive content.* Google provides users with a certain amount of free "cloud" storage, currently 15 gigabytes, through a service called "Google Drive" (users can purchase a storage plan through Google to store additional content). Users can purchase enhanced storage capacity for an additional monthly fee. Users can use their Google Drive to store email, attachments, videos, photographs, documents, and other content "in the cloud," that is online. A user can access content stored on Google Drive by logging into his or her Google account through any computer or other electronic device that is connected to the Internet. Users can also share files stored on Google Drive with others, allowing them to view, comment, and/or edit the files.

x. *Google Docs.* Google provides users with the ability to write, edit, and collaborate on various documents with other Google users through a service called "Google Docs." Users can use Google Docs to create online documents that can be stored on, or saved to the user's Google Drive.

xi. *Google Photos.* Google provides users with a certain amount of free storage for photographs, through a service called Google Photos, which

allows users to manually store photographs and videos, and which automatically uploads photographs and videos taken by registered mobile devices. Google also retains the metadata---or data that provides information about the data in question, such as the time and date of creation, the author or creator, the means of its creation, the purpose of the data, among other data---for photos and videos that are uploaded to Google, including to Google Photos. This metadata includes what is known as exchangeable image file format (or "Exif") data, and can include GPS location information for where a photo or video was taken.

xii. *Google Calendar.* Google provides users with an online calendar, in which they can add appointments, events, and reminders, which are synchronized across registered computer and mobile devices. Users can share their calendars with other users, allowing the maintenance of joint calendars.

xiii. *Google Chats and Google Hangouts content.* Google allows subscribers to engage in "chat" sessions in an instant messaging format with other Google users, the transcripts of which are generally stored in a user's email content. Similarly, Google allows users to engage in enhanced chat sessions, called Hangouts, which permit the sharing of additional content such as videos, sounds, and images. In general, Hangouts content is stored separately from a user's email and chat content.

xiv. *Location History Data.* Google maintains recent location data, collected periodically, from mobile devices that are logged into or have used

applications (or "apps") or services provided by Google. For example, Google collects information collected from GPS (global positioning system), Wi-Fi networks, cell site locations, and mobile networks to estimate a user's location. Google apps and services also allow for location reporting, which allows Google to periodically store and use a device's most recent location data in connection with a Google account.

xv. *Google Payments.* Google allows for the storage of payment information associated with a Google Account, including credit cards and ban k accounts, and contains information about all transactions made with a Google account, allowing for the payment for goods (such as those purchased through Google Shopping) and bills, among other features.

xvi. *Google Plus.* Google hosts and Internet-based social network. Among other things, users can post photos and status updates and group different types of relationships (rather than simply "friends") into Circles. In addition, Google has a service called PlusOne, in which Google recommends links and posts that may be of interest to the account, based in part on accounts in the user's Circle having previously clicked "+1" next to the post. PlusOne information therefore provides information about the user of a given account, based on activity by other individuals the user has entered in the user's Circle.

xvii. *Chrome Browser and Search History.* Google stores information regarding user Internet browser activity when a Google user is logged into his or account, which includes logging information about websites viewed

by the user, Internet search queries in the Google Internet search engine available at http://www.google.com, and also maintains lists of bookmarks maintained by the user so that he or she can quickly access frequently viewed websites.

xviii. *Advertising Data.* Google also stores advertising data, including information regarding unique advertising IDs associated with the customer, devices used to access the account, application IDs, Android IDs, advertising cookies, Unique Device Identifiers (UDIDs), payment information, ads clicked, and ads created.

xix. *YouTube Data.* Google owns the video-streaming service YouTube and maintains records relating to YouTube accesses and data posted by the user.

xx. *Google Analytics.* Google Analytics is a web analytics service that tracks and reports website traffic. *See* http://support.google.com/analytics/?hl=en#topic=3544907. According to Google, it allows for data collection and management, including the following features: (1) an open measurement protocol for comprehensive data collection that can be used to import interaction data from any internet-connection third-party system into Google Analytics; and (2) the ability to "upload data from external sources and combine it with data collected via Google Analytics to extend and cleanse existing data." *See* http://www.google.com/analytics/analytics/features. According to Google, Google Analytics also allows for data analysis, visualization, and

reporting, including the following features: (1) user flow reporting that allows the user to see how visitors flow throughout a website; and (2) real-time reporting regarding website accesses. *Id.* Furthermore, according to Google, Google Analytics allows for data activation, including the ability to obtain demographic and interest data to understand the ages and genders of the website users. *Id.* Google stores the property ID associated with a Google Analytics account, which refers to the website or application which the user would track. Google also stores all user accounts associated with a property ID. An Analytics tracking code (or"UA code") collects data with respect to a given web property, and returns that data to Analytics where the user can see it in reports. When a user adds a new web property to his or her Analytics account, Analytics generates the tracking code snippet that is needed to add to the pages whose data the user wants to collect. The user can then use this tracking code snippet as is, or customize it to collect additional data. The tracking code snippet contains a unique ID for the web property that lets the user identify that property's data in his or her reports. Google Analytics can generate a wide variety of reports, which it stores with respect to a given UA property ID, including Audience Reports. Audience Reports include information on a variety of factors, including the types of mobile devices being used to interact with a property and geographic information regarding devices that browse to a property, which could provide some

information regarding the identity of the individuals who access a website, including co-conspirators who access a website.

xxi. *Google Developer Console.* Based on Google's website (http://developers.google.com), Google offers several "Developer Consoles," including Google API Console, Google Cloud Platform Console, Firebase Console, Case SDK Developer Console, and Chrome Web Store Dashboard. These consoles can be used, among other things, to develop software and application programming interfaces (APIs").

27. I have learned the following about WhatsApp.

a. WhatsApp is a cross-platform mobile messaging application which allows a user to exchange messages without having to pay service fees for use. WhatsApp is available for use as an application on an iPhone, Blackberry, Android, Windows-based or Nokia telephone. WhatsApp does not use traditional cellular or wire communication lines for communications, but instead relies on internet access for communication. Users are required to subscribe to WhatsApp by using their mobile phone number an they are able to operate the application in a manner consistent with traditional mobile telephone use. Upon subscription, the WhatsApp Messenger confirms subscription by transmitting a message to the subscriber's telephone number.

b. Specifically, the WhatsApp application allows its subscribers to communicate with other subscribers to the application or with subscribers to related third-party applications and websites using the following features: (1) instant messaging, (2) text, picture, video, and audio media messaging, (3) group chat; (4) status

updates; and (5) geolocation sharing. WhatsApp also allows subscribers to store an address list of WhatsApp accounts. Additionally, WhatsApp maintains records of the WhatsApp groups of which a subscriber is a member, including the identification of other WhatsApp accounts in the group, the group's name, and any photograph associated with the group. Furthermore, WhatsApp maintains subscriber records for WhatsApp accounts, which may include the user's phone number, email, and IP addresses used to access the account. WhatsApp may also maintain device information.

28. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and experience, I know that, even if subscriber's insert false information to conceal their identities, this information often provides clues to their locations, identities, and illicit activities.

29. In my training and experience, evidence of who was using an account, and from where, and evidence related to criminal activity of the kind described below, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. The stored communications and files connected to an account may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, and videos are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

30. In addition, the user's account activity, logs, stored communications, and other data retained by Facebook, Google, and WhatsApp can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a residential search warrant.

31. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate that owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement). Such activity can include Google searches relating to crime.

32. Other information connected to a Facebook, Google, or WhatsApp account may lead to the discovery of additional evidence. For example, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation. This is particularly important in a case such as this one, wherein the subject may have made efforts to obfuscate their illegal activities and to avoid detection from law enforcement.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

33. Your Affiant will execute this search warrant pursuant to the provisions of the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the search warrant to require Facebook, Google, and WhatsApp to disclose to the government copies of the records and other information (including the content of communications) set forth in Section I of Attachment B. Upon receipt of the information

described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

34. Based on the forgoing, I request that the Court issue the proposed search warrants to Facebook, Google, and WhatsApp because there is probable cause to believe evidence is stored at the premises controlled by Facebook, Google, and WhatsApp pertaining to an ongoing criminal investigation in the Western District of Arkansas, Hot Springs Division and elsewhere, of violations of 18 U.S.C. § § 2251 (production of child pornography), 2252 (distribution of child pornography) and 1591(a)(1) (sex trafficking of a person who has not attained the age of 18 years).

35. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

REQUEST FOR SEALING

36. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize the ongoing investigation.

Respectfully submitted,

Katie C. Rowbotham, Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on February 21, 2019

Honorable Barry A. Bryant
United States Magistrate Judge

ATTACHMENT A1

Property to Be Searched

This warrant applies to information associated with the Facebook user ID's: **100026170149068, 100013269482917, 100009344742059, 100025340801469, 100028908998220**, **100024430478019,** and **100014475964292** that is stored at premises owned, maintained, controlled, or operated by Facebook Inc., a company headquartered in Menlo Park, California.

ATTACHMENT A2

Property to Be Searched

This warrant applies to information associated with the Google accounts allooper2600@gmail.com and allhiswill2600@gmail.com, that are stored at premises owned, maintained, controlled, or operated by Google LLC, an electronic communication service provider located in Mountain View, California.

ATTACHMENT A3

Property to Be Searched

This warrant applies to information associated with the WhatsApp accounts with allooper2600@gmail.com and allhiswill2600@gmail.com that are stored at premises owned, maintained, controlled, or operated by WhatsApp, an electronic communication service provider located in Menlo Park, California.

ATTACHMENT B1

Particular Things to be Seized

I. Information to be disclosed by Facebook

To the extent that the information described in Attachment A1 is within the possession, custody, or control of Facebook Inc. ("Facebook"), regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for the user ID listed in Attachment A1:

(a) All contact and personal identifying information, including for Facebook user ID's: **100026170149068, 100013269482917, 100009344742059, 100025340801469, 100028908998220, 100024430478019,** and **100014475964292:** full name, user identification number, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.

(b) All activity logs for the account and all other documents showing the user's posts and other Facebook activities from January 1, 1999 to present.

(c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them from January 1, 1999 to present, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos;

(d) All profile information; News Feed information; status updates; videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including

the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

(e) All records or other information regarding the devices and internet browsers associated with, or used in connection with, that user ID, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string;

(f) All other records and contents of communications and messages made or received by the user from January 1, 1999 to present, including all Messenger activity, private messages, chat history, video and voice calling history, and pending "Friend" requests;

(g) All "check ins" and other location information;

(h) All IP logs, including all records of the IP addresses that logged into the account;

(i) All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";

(j) All information about the Facebook pages that the account is or was a "fan" of;

(k) All past and present lists of friends created by the account;

(l) All records of Facebook searches performed by the account from January 1, 1999 to present;

(m) All information about the user's access and use of Facebook Marketplace;

(n) The types of service utilized by the user;

(o) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

(p) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;

(q) All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

Facebook is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

ATTACHMENT B2

Particular Things to be Seized

II. Information to be disclosed by Google

To the extent that the information described in Attachment A2 is within the possession, custody, or control of Google Inc., regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Google, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google is required to disclose the following information to the government for the user ID listed in Attachment A2:

(a) The content of all communication that went to or from the account (including through Gmail, Google Hangouts (including videos), and otherwise), stored in draft form in the account, or otherwise associated with the account, including all message content, attachments, and header information;

(b) All address book, contact list, or similar information associated with the account;

(c) Full Google search history and Chrome history associated with the account;

(d) All Google Drive content;

(e) All bookmarks maintained by the account;

(f) All services used by the account;

(g) All subscriber and payment information, including full name, e-mail address (including any secondary or recovery email addresses), physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, telephone number, website, screen names, user identification numbers, security

questions and answers, registration IP address, payment history, and other personal identifiers;

(h) All past and current usernames, account passwords, and names associated with the account;

(i) The dates and times at which the account and profile were created and the Internet Protocol ("IP") address at the time of sign-up;

(j) All YouTube data associated with the account;

(k) All transactional records associated with the account; including any IP logs or other records of session times and durations;

(l) Any information identifying the device or devices used to access the account, including a device serial number, a GUID or Global Unique Identifier, Android ID, phone number, serial numbers, MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Equipment Identities ("IMEI"), and any other information regarding the types of devices used to access the account;

(m) All activity logs for the account;

(n) All photos and videos uploaded to the account, including in Google Drive and Google Photos;

(o) All information associated with Google Plus, including the names of all Circles and the accounts grouped into them;

(p) Google Analytics; All properties and UA codes associated with the accounts, and for each of those properties and UA codes, all usernames and email accounts associated with them. In addition, for all properties and UA codes associated with the accounts, all audience reports. All data uploaded by the user of accounts into Google Analytics.

(q) All photos and videos uploaded by any user that have that user tagged in them;

(r) All location and maps information;

(s) All Google Voice information;

(t) The length of service (including start date) and the means and source of payments associated with the service (including any credit card or bank account number);

(u) All privacy settings and other account settings, including email addresses or other accounts that the account has blocked;

(v) Advertising and Device Data; All advertising data relating to the account, including, but not limited to, advertising cookies, information regarding unique advertising IDs associated with the user, any devices used to access the account, Android IDs, application IDs, UDIDs, payment information (including, but not limited to, full credit card numbers and expiration dates and PayPal accounts), ads clicked, and ads created;

(w) Linked Accounts; All accounts linked to the provided accounts (including where linked by machine cookie or other cookie, creation or login IP address, recovery email or phone number, AOL account ID, Android ID, Google ID, SMS, Apple ID, or otherwise);

(x) For accounts linked by cookie, the date(s) on which they shared a cookie;

(y) For accounts linked by SMS number, information regarding whether the numbers were verified; and

(z) Customer Correspondence; All records pertaining to communications between the Service Provider and any person regarding the user of the user's account with the Service Provider, including contacts with support services, records of actions taken, and investigative or user complaints concerning the subscriber.

ATTACHMENT B3

Particular Things to be Seized

III. Information to be disclosed by WhatsApp

To the extent that the information described in Attachment A3 is within the possession, custody, or control of WhatsApp, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to WhatsApp, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), WhatsApp is required to disclose the following information to the government for the user ID listed in Attachment A3:

(a) All identity and contact information, including full name, e-mail address, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers;

(b) All past and current usernames, account passwords, names and telephone numbers associated with the account;

(c) The dates and times at which the account and profile were created, and the Internet Protocol ("IP") address at the time of sign-up;

(d) All IP logs and other documents showing the IP address, date, and time of a subscribers use of the account;

(e) All data and information associated with any user profile, including photographs, "bios" and profile backgrounds and themes;

(f) All photographs and images associated with the subscriber's account;

(g) All location data associated with the account, including geolocation sharing information with other accounts;

(h) All data and information that has been deleted by the user;

(i) A list of all people, telephone numbers or accounts that are linked to the WhatsApp account, including through third-party applications or websites, along with the identity and contact information for each linked person, telephone number and account, including full name, e-mail address, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers;

(j) All privacy and account settings;

(k) All information about connections between the account and third-party websites and applications;

(l) All records pertaining to communications between WhatsApp and any person or account regarding the user or the user's WhatsApp account, including contacts with support services, and all records of actions taken, including suspensions of the account;

(m) All communications between WhatsApp and the account;

(n) All communications between the account and any other WhatsApp account or associated third-party website or application account including all retained (1) instant messaging, (2) text, picture, video, and audio media messaging, (3) group chats, (4) status updates; and (5) geolocation sharing information;

(o) All address book data; and

(p) All group data, including, for each group, the group's membership report, and for each group, the group profile report, including the identifier, creation date, number of participants, group name, and all associated images.

IV. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, and Sections 1591 and 875 involving Aaron Looper since January 1, 1999 including, for the user ID's identified on Attachment A, information pertaining to the following matters:

(a) Message communications between Facebook, Google and WhatsApp user accounts and other users, known or unknown, where pictures were received and/or traded.

(b) The identity and whereabouts of those persons who created, used, or communicated with the Facebook, Google, and WhatsApp accounts identified in Attachment A.

(c) Evidence indicating how and when the Facebook, Google, and WhatsApp accounts were accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the account owner;

(d) Evidence indicating the Facebook, Google, and WhatsApp account owner's state of mind as it relates to the crime under investigation;

(e) The identity of the person(s) who created or used the user ID's, including records that help reveal the whereabouts of such person(s).